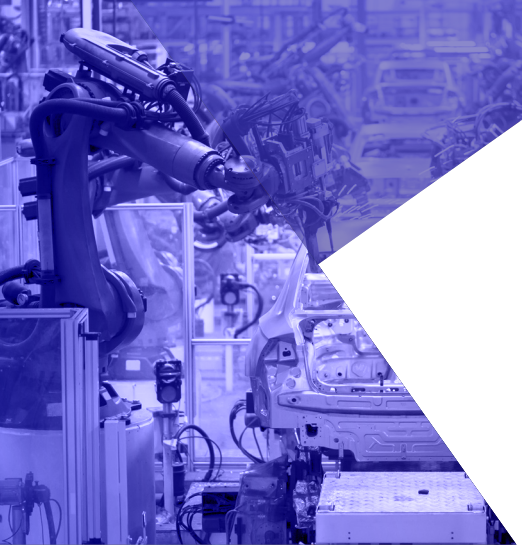


Industry
Manufacturing

Attacker Objective
Profit from holding files for ransom

Awake detected this threat by:

- Detecting ransomware TTPs such as credential abuse, privilege escalation and lateral movement.
- Identifying the disabling of security measures such as Microsoft's User Account Control.
- Uncovering the use of PowerShell for ransomware distribution.

Ransomware Attack Unfolds

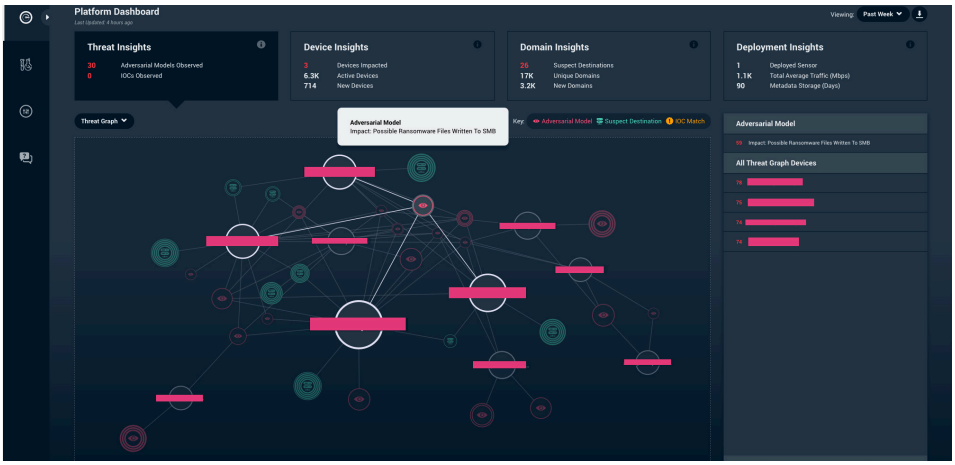
In September 2019, Awake was engaged in a Proof of Value trial with a manufacturing company at their Dallas, TX location.

While the customer was evaluating the Awake Security Platform, a company facility in Atlanta, GA was hit by a ransomware attack. The Sodinokibi ransomware executed and encrypted more than 2,500 files, effectively shutting down four of the company's critical servers. The attacker demanded $750,000 ransom for the files.

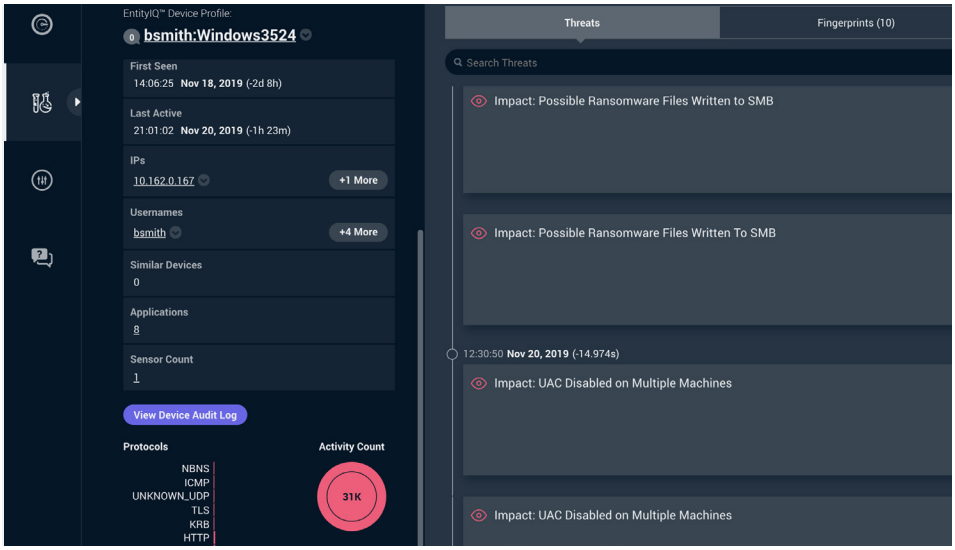
While this attack was unfolding in Atlanta, Awake identified suspicious logins with a legitimate (but what appeared to be a compromised) admin account.

Purely through network traffic analysis, Awake notified the security team that the attacker had disabled User Account Control, a key Microsoft Windows security feature, on all machines on the network. The Awake Security Platform also identified 39 devices connecting to PasteBin using PowerShell, in what appeared to be an attempt to download the next stage of the ransomware. Finally, Awake identified lateral movement attempts from the infected devices in Atlanta to the Dallas location being monitored by Awake.

Awake's identification of the tactics, techniques and procedures (TTPs) such as credential abuse, privilege escalation and lateral movement used by ransomware threat actors, prevented the attack from spreading to the Dallas location. The full attack was thus stopped in its tracks and the damage was minimized to just the unmonitored Atlanta location.



Awake's Threat Insights dashboard highlights the attempts to spread the ransomware.



Awake highlights the threat timeline as the ransomware attempted to spread to the environment in Dallas.

For additional information about Awake please visit awakesecurity.com

AWAKE